REMARKS:

This paper is herewith filed in response to the Examiner's Office Action mailed on January 4, 2007 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-14 of the application.

More specifically, the Examiner has rejected claims 1-14 under 35 USC 102(e) as anticipated by Win et al. (US6,453,353). The applicant respectfully disagrees with the rejections.

Claim 1 recites:

> A method for authorizing a network device, comprising: determining an attribute based, in part, on a capability of the network device; generating an attribute certificate based, in part, on the attribute; storing the attribute certificate including the attribute; and if the attribute certificate is valid, authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate.

In the reference Win et al. as cited in the rejection of claim 1, the Examiner appears to identify wherein "the browser sends an open URL request and cookie to a Protected Web Server," (col. 6, lines 58-59) as anticipating "determining an attribute based, in part, on a capability of the network device," as in claim 1. However, in Win et al. the cookie "is a packet of data sent by web servers to web browsers" (col. 6, lines 47-48), and "Cookies received from a web server in a specific domain are returned to web servers in that same domain during open URL requests," (col. 6, lines 49-51). In Win et al. "A cookie returned by the Authentication Client Module is required for access to resources protected by the system 2," (col. 6, 51-53). Clearly, the cookie as provided by the web server in Win et al. does not anticipate the "attribute based, in part, on a capability of the network device," as in claim 1.

In Win et al. "The Authentication Client Module authenticates a user by verifying the name and password with the Registry Server 108," (col. 6, lines 41-43). Then "If the name and password

are correct, the Authentication Client Module reads the user's roles from the Registry Server 108," and "It then encrypts and sends this information in a "cookie" to the user's browser," (col. 6, lines 43-47). Clearly, a "user's roles" as determined from the user name and password in Win et al. is not seen as being equivalent to the capability of a network device. Therefore, the Applicant asserts that in Win et al. the cookie which is created as a result of a user authentication is seen as entirely distinguishable from the attribute certificate which is based in part on the capabilities of the network device as in the claimed invention. For at least this reason the Applicant contends that Win et al. does not disclose or suggest "authorizing a network device, comprising: determining an attribute based, in part, on a capability of the network device" as in claim 1.

Furthermore, the background section of the written description recites a similar method of authentication as in Win et al. wherein "Kerberos tickets provide a means for applications to share cryptographically authenticated credential among several applications," (page 1, lines 15-16). Motivation for the claimed invention over the prior art is disclosed as "Kerberos tickets only indicate that a particular user has successfully authenticated to a central network server, thereby establishing a single user session," (page 1, lines 17-18). The Applicant contends that Win et al. is seen to disclose a similar method as described in the background of the claimed invention. In Win et al., "Preferably, the cookies are encrypted rather than digitally signed because encryption is faster and produces a smaller cookie" (col. 10, lines 59-61), and "The cookies 528, 530 are passed to each Web server that the user accesses and that is within the same domain as the Access Server 106," (col. 10, line 67 to col. 11, line 2). In Win et al. "The system 2 also enables Users to log-in to the system once, and thereafter access one or more Resources during an authenticated session," (col. 5, line 66 to col. 6, line 1). As Win et al. discloses, "the system provides a mechanism of single secure log-in to Web resources,"(col. 6, lines 7-9). As the method of Win et al. appears to be analogous to the prior art as disclosed in the claimed invention, it is apparent that Win et al. does not anticipate the claimed invention.

Therefore for at least the reasons stated Win et al. does not disclose or suggest claim 1 and claim 1 should be allowed.

With regards to the rejection of claim 2, the Examiner states that "Win teaches attribute is further determined based, in part on an automated security scan of the network device (abstract, col. 5, line 55-col. 6, line 10, col. 10, lines 34-67). The Applicant respectfully disagrees with the Examiner.

The Applicant can find no support in Win et al. to disclose or suggest "an automated scan of the network device," as in claim 2. The most applicable reference as cited by the Examiner merely discloses "after the Authorization service of Authentication Client module 414 has looked up a user's roles from the Registry Server 108, Access Menu Module 412 uses a Personalized Menu Service to build a list of resources 208 that are available to the user" and "Access Server 106 determines that the user is authentic, using the steps described above, and requests Registry Server 108 to return a profile of the user," (col. 11, lines 44-48). Then "As shown by state 542, the personalized menu is returned to the browser 100 in the form of a Web page or HTML document," (col. 11, lines 60-62). The reference as cited does not disclose or suggest "wherein the attribute is further determined based, in part, on an automated security scan of the network device," as disclosed in claim 2. Also as the dependent claim 11 recites a similar feature of claim 2, neither claim 2 nor claim 11 is disclosed or suggested in the reference as cited.

The Applicant respectfully requests clarification of the rejection in a non-final office action or an allowance of claim 2 and claim 11.

In the rejection of claim 14 the Examiner states "Win teaches a network device for managing authorization to a resource over a network, comprising: a means for generating an attribute certificate, wherein the attribute certificate is based on a capability of another network device (abstract, Figure 1, col. 6, lines 58-65, col. 11, line 42-col. 12, line 8)." The Applicant respectfully disagrees and traverses the rejection.

As stated above, in Win et al. "The Authentication Client Module authenticates a user by verifying the name and password with the Registry Server 108," (col. 6, lines 41-43). Therefore,

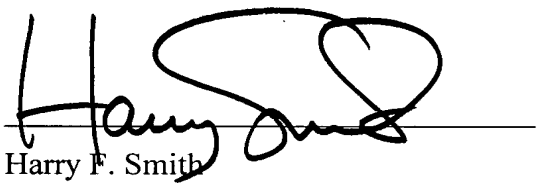
in Win et al. the cookie is created as a result of a user authentication, wherein the claimed invention "the attribute certificate is based on a capability of another network device," as claim 14 recites in part. Further, in Win et al. "The Registry Server manages access to the Registry Repository," (col. 12, lines 10-11), and the Registry Server "stores User, Resource, and Role information," (col. 12, line 16). Clearly, Win et al. does not disclose "generating an attribute certificate, wherein the attribute certificate is based on a capability of another network device," and so does not disclose or suggest "a means for storing the attribute certificate," that is generated as claimed in claim 14. Win et al. merely discloses in part a method to manage "cookies" created as a result of user authentication. Thus, for at least the reasons stated Win et al. does not disclose or suggest claim 14, and claim 14 should be allowed.

In addition, as the independent claim 9 recites a similar feature of claim 1, for at least the reasons stated above Win et al. does not anticipate these claims, and all the claims 1, 2, 9, 11 and 14 should be allowed.

Furthermore, as the claims 2-8, 10-13, depend from claims 1 and 9 respectively, Win et al. does not anticipate these claims, and all the claims 1-14 should be allowed.

Based on the above explanations and arguments, it is clear that Win et al. cannot be seen to anticipate claims 1-14. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1-14 under 35 U.S.C. §102(e) and to allow all of the pending claims 1-14 as presented for examination. For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' agent at the telephone number indicated below.

Respectfully submitted:



4/3/2007

Harry F. Smith — Date

Reg. No.: 32,493

Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Phone: (203) 925-9400
Facsimile: (203) 944-0245
Email: hsmith@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Ann Okrentowich — 4-3-07

Name of Person Making Deposit — Date